

AO 93 (Rev. 01/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Northern District of California

JSC

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Case No. 3 19 71763

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH)
MCHOY.SCM@GMAIL.COM; JOSH.CLARK@HAMMERTXAS.COM;)
JS@TRFPI.COM; JH@TRFPI.COM; CV@TRFPI.COM;)
JSTANKA@GMAIL.COM)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

See Attachments A-1 and A-2

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachments B-1 and B-2

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

11/11/2019

(not to exceed 10 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

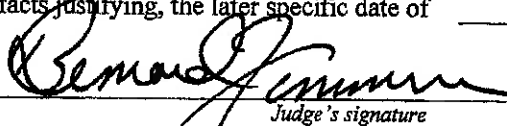
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

Hon. Bernard Zimmerman

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ Until, the facts justifying, the later specific date of _____.

Date and time issued: 25 Oct 2019 at 2:47pm


Judge's signatureCity and state: San Francisco, California

Hon. Bernard Zimmerman, United States Magistrate Judge

Printed name and title

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A-1
PROPERTY TO BE SEARCHED

This warrant applies to information associated with the account:

- **mchoy.scm@gmail.com**
- **josh.clark@hammertexas.com**
- **js@trfpi.com**
- **jh@trfpi.com**
- **cv@trfpi.com**

that are stored at premises controlled by Google, LLC a company headquartered at
1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT A-2
PROPERTY TO BE SEARCHED

This warrant applies to information associated with the account:

- **jstanka@gmail.com**

that are stored at premises controlled by Google, LLC a company headquartered at
1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B-1

PARTICULAR THINGS TO BE SEIZED

To ensure that agents search only account(s) described in Attachment A-1, this search warrant seeks authorization to permit employees of Google, LLC (the "Provider") to assist agents in the execution of the warrant. To further ensure that agents executing this warrant search only the accounts described as **mchoy.scm@gmail.com**, **josh.clark@hammertexas.com**, **js@trfpi.com**, **jh@trfpi.com**, and **cv@trfpi.com**, the following procedures have been implemented:

I. Search Procedure

The search warrant will be presented to Google, LLC's personnel, who will be directed to isolate those accounts and files described in Section II below:

1. In order to minimize any disruption of computer service to innocent third parties, Google, LLC's employees will create an exact duplicate of the accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein;
2. Law enforcement personnel will thereafter review the information received stored and identify and copy only the information authorized to be further copied as described in Section III below; and
3. Law enforcement personnel will then seal the original duplicate of the accounts and files received from Google, LLC's employees and will not further review the original duplicate absent an order of the Court.

In the review of information provided pursuant to this warrant by Google, LLC, the government must make reasonable efforts, to the extent required by the Fourth Amendment, to use methods and procedures that will locate and expose those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant while minimizing exposure or examination of irrelevant or attorney-client privileged files to the extent reasonably practicable.

//

II. Files and Accounts to be Copied by Provider's Employees

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Google, LLC, regardless of whether such information is located within or outside of the United States, and including any chats, records, files, logs, or information that has been deleted but is still available to Google, LLC or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, LLC is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

1. The contents of all emails and chat sessions stored in the account from January 1, 2014 to the present, including copies of emails and chats sent to and from the account, draft emails/chats, the source and destination addresses associated with each email/chat, the date and time at which each email/chat was sent, and the size and length of each email/chat;
2. All records or other information regarding the identification of the account, including full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
3. All subscriber records for the account;
4. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, documents, and files;
5. All records associated with the uploading, sending, and receipt of images, documents, and files, including all time and date stamps, device information, and IP addresses for each interaction;
6. All records pertaining to communications between Google, LLC and any person regarding the account, including contacts with support services and records of actions taken; and
7. All records or other information regarding the user's account settings.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

III. Information to be Further Copied by Law Enforcement Personnel

All information described above in Section II that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 U.S.C. Section 286 (Conspiracy to Defraud the United States by False Claims), Title 18, U.S.C. Section 550 (False Claim for Refund of Duties), Title 18, U.S.C. Section 1341 (Mail Fraud), Title 18 U.S.C. Section 1343 (Wire Fraud); Title 18 U.S.C. Section 1956(h) (Conspiracy to Launder Money); and Title 18 U.S.C. Section 1957 (Money Laundering) those violations involving owners, employees, or contractors of Pacific Rim Traders, LLC, ML Trading Group, Inc., Bay Area Tire Recycling Inc., Asian International Trading, TPP Export America, LLC, Trans Pacific Polymers, LLC, Hammer Trading, LLC, Tariff Partners International LLC, Margaret Palacios, Dale Behm, Neill Stroth, Sarah Stroth, Villfredy Alvarenga, Yong Heng (Colin) Liang, Brian Henkels, Joshua Stanka, Joshua Clark, David Burbidge, and Michael Choy (the co-conspirators) occurring between January 1, 2014 and the present, specifically, for the account or identifier listed on Attachment A-1, information pertaining to the following matters:

1. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, information necessary to prepare drawback claims, documentation and support material of imports or exports, invoices, bills of lading, other shipping related documents.
2. Communications between co-conspirators and others that discuss or otherwise show the user(s) of the target account and any company or entity affiliation or employment of that person or persons, and that of other members of the conspiracy and their respective roles and actions in furtherance of the scheme.
3. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, knowledge of drawback regulations, the harmonized

tariff schedule, or Department of Homeland Security and Customs and Border Protection regulations and requirements.

4. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, modification or knowledge of modification of bills of lading, invoices, contents of containers, shipping documents, duty drawback claim documents, and exported materials.
5. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, the preparation of company books and records, the preparation of personal income tax returns, business income tax returns, refund amounts, methods of payment, bank account information, status of prepared and/or filed income tax returns, and knowledge of income tax laws and regulations.
6. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, information regarding the acquisition and distribution of funds received from the violations listed above, including bank account information, commission payments, bank account set up instructions, individuals listed with access to bank accounts, method of deposits, acceptance from federal authorities, and information regarding individuals with ability and access to virtually deposit checks.
7. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, information regarding agreements and business contracts between co-conspirators and others, including monetary agreements and non-monetary agreements.
8. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, personal identifying information, names, routing numbers, bank account numbers, addresses, dollar amounts, Moneygram, Western Union, MoneyPak, wiring instructions, pre-paid debit cards, or any other details related to financial accounts or financial transactions.

9. Records that show who created, used, or communicated with the account, including records about their identities and whereabouts, insofar as this information constitutes evidence of a violation of Title 18 U.S.C. Section 286 (Conspiracy to Defraud the United States by False Claims), Title 18, U.S.C. Section 550 (False Claim for Refund of Duties), Title 18, U.S.C. Section 1341 (Mail Fraud), Title 18 U.S.C. Section 1343 (Wire Fraud); Title 18 U.S.C. Section 1956(h) (Conspiracy to Launder Money); and Title 18 U.S.C. Section 1957 (Money Laundering).
10. Identification of other accounts, domains, IP addresses, and computers owned or controlled by the same individual(s) controlling each account listed at Attachment A-1; and the following documents that tend to establish the identity of the person or persons in control of the account: identification documents (such as driver's licenses or passports), photographs, bills, receipts, vehicle registration documents, statements, leasing agreements, personal address books, calendars, daily planners, and personal organizers.

ATTACHMENT B-2

PARTICULAR THINGS TO BE SEIZED

To ensure that agents search only account(s) described in Attachment A-2, this search warrant seeks authorization to permit employees of Google, LLC (the "Provider") to assist agents in the execution of the warrant. To further ensure that agents executing this warrant search only the account described as **jstanka@gmail.com** the following procedures have been implemented:

I. Search Procedure

The search warrant will be presented to Google, LLC's personnel, who will be directed to isolate those accounts and files described in Section II below:

1. In order to minimize any disruption of computer service to innocent third parties, Google, LLC's employees will create an exact duplicate of the accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein;
2. Law enforcement personnel will thereafter review the information received stored and identify and copy only the information authorized to be further copied as described in Section III below; and
3. Law enforcement personnel will then seal the original duplicate of the accounts and files received from Google, LLC's employees and will not further review the original duplicate absent an order of the Court.

In the review of information provided pursuant to this warrant by Google, LLC, the government must make reasonable efforts, to the extent required by the Fourth Amendment, to use methods and procedures that will locate and expose those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant while minimizing exposure or examination of irrelevant or attorney-client privileged files to the extent reasonably practicable.

//

II. Files and Accounts to be Copied by Provider's Employees

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Google, LLC, regardless of whether such information is located within or outside of the United States, and including any chats, records, files, logs, or information that has been deleted but is still available to Google, LLC or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, LLC is required to disclose the following information to the government for each account or identifier listed in Attachment A-2:

1. The contents of all emails and chat sessions stored in the account from January 1, 2018 to the present, including copies of emails and chats sent to and from the account, draft emails/chats, the source and destination addresses associated with each email/chat, the date and time at which each email/chat was sent, and the size and length of each email/chat;
2. All records or other information regarding the identification of the account, including full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
3. All subscriber records for the account;
4. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, documents, and files;
5. All records associated with the uploading, sending, and receipt of images, documents, and files, including all time and date stamps, device information, and IP addresses for each interaction;
6. All records pertaining to communications between Google, LLC and any person regarding the account, including contacts with support services and records of actions taken; and
7. All records or other information regarding the user's account settings.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

III. Information to be Further Copied by Law Enforcement Personnel

All information described above in Section II that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 U.S.C. Section 286 (Conspiracy to Defraud the United States by False Claims), Title 18, U.S.C. Section 550 (False Claim for Refund of Duties), Title 18, U.S.C. Section 1341 (Mail Fraud), Title 18 U.S.C. Section 1343 (Wire Fraud); Title 18 U.S.C. Section 1956(h) (Conspiracy to Launder Money); and Title 18 U.S.C. Section 1957 (Money Laundering) those violations involving owners, employees, or contractors of Pacific Rim Traders, LLC, ML Trading Group, Inc., Bay Area Tire Recycling Inc., Asian International Trading, TPP Export America, LLC, Trans Pacific Polymers, LLC, Hammer Trading, LLC, Margaret Palacios, Dale Behm, Neill Stroth, Sarah Stroth, Villfredy Alvarenga, Yong Heng (Colin) Liang, Brian Henkels, Joshua Stanka, Joshua Clark, David Burbidge, and Michael Choy (the co-conspirators) occurring between January 1, 2018 and the present, specifically, for the account or identifier listed on Attachment A-2, information pertaining to the following matters:

1. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, information necessary to prepare drawback claims, documentation and support material of imports or exports, invoices, bills of lading, other shipping related documents.
2. Communications between co-conspirators and others that discuss or otherwise show the user(s) of the target account and any company or entity affiliation or employment of that person or persons, and that of other members of the conspiracy and their respective roles and actions in furtherance of the scheme.
3. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, knowledge of drawback regulations, the harmonized tariff schedule, or Department of Homeland Security and Customs and Border Protection regulations and requirements.

4. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, modification or knowledge of modification of bills of lading, invoices, contents of containers, shipping documents, duty drawback claim documents, and exported materials.
5. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, the preparation of company books and records, the preparation of personal income tax returns, business income tax returns, refund amounts, methods of payment, bank account information, status of prepared and/or filed income tax returns, and knowledge of income tax laws and regulations.
6. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, information regarding the acquisition and distribution of funds received from the violations listed above, including bank account information, commission payments, bank account set up instructions, individuals listed with access to bank accounts, method of deposits, acceptance from federal authorities, and information regarding individuals with ability and access to virtually deposit checks.
7. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, information regarding agreements and business contracts between co-conspirators and others, including monetary agreements and non-monetary agreements.
8. Communications between co-conspirators and others that discuss or otherwise show, in coded or un-coded language, personal identifying information, names, routing numbers, bank account numbers, addresses, dollar amounts, Moneygram, Western Union, MoneyPak, wiring instructions, pre-paid debit cards, or any other details related to financial accounts or financial transactions.
9. Records that show who created, used, or communicated with the account, including records about their identities and whereabouts, insofar as this information constitutes evidence of a violation of Title 18 U.S.C. Section 286 (Conspiracy to Defraud the

United States by False Claims), Title 18, U.S.C. Section 550 (False Claim for Refund of Duties), Title 18, U.S.C. Section 1341 (Mail Fraud), Title 18 U.S.C. Section 1343 (Wire Fraud); Title 18 U.S.C. Section 1956(h) (Conspiracy to Launder Money); and Title 18 U.S.C. Section 1957 (Money Laundering).

10. Identification of other accounts, domains, IP addresses, and computers owned or controlled by the same individual(s) controlling each account listed at Attachment A-2; and the following documents that tend to establish the identity of the person or persons in control of the account: identification documents (such as driver's licenses or passports), photographs, bills, receipts, vehicle registration documents, statements, leasing agreements, personal address books, calendars, daily planners, and personal organizers.